(v) Radio and telecommunication systems, including computer systems and networks; and

(vi) Essential services.

(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) OCS facility personnel;

(ii) Visitors, vendors, repair technicians, vessel personnel, etc.;

(iii) OCS facility stores;

(iv) Any security communication and surveillance systems; and

(v) Any other security systems, if any.

(4) The FSA report must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between personnel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The FSA report must discuss and evaluate key OCS facility measures and operations, including—

(i) Ensuring performance of all security duties;

(ii) Controlling access to the OCS facility through the use of identification systems or otherwise;

(iii) Controlling the embarkation of OCS facility personnel and other persons and their effects (including personal effects and baggage, whether accompanied or unaccompanied);

(iv) Supervising the delivery of stores and industrial supplies;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the OCS facility; and

(vii) The ready availability of security communications, information, and equipment.

(e) The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure.

[USCG–2003–14759, 68 FR 39345, July 1, 2003; 68 FR 41917, July 16, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

§ 106.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan (FSP) required in § 106.410 of this part.

(b) An OCS facility owner or operator may generate and submit a report that contains the FSA for more than one OCS facility subject to this part, to the extent that they share similarities in physical characteristics, location and operations.

(c) The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for reapproval or revisions.

[USCG–2003–14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60558, Oct. 22, 2003]

Subpart D—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

§ 106.400 General.

(a) The OCS facility owner or operator must ensure the FSO develops and implements a Facility Security Plan (FSP) for each OCS facility for which he or she is designated as FSO. The FSP:

(1) Must identify the FSO by name or position and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Facility Security Assessment (FSA);

(4) Must describe security measures for each MARSEC Level; and

(5) May cover more than one OCS facility to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the cognizant District Commander.

(b) The FSP must be submitted for approval to the cognizant District Commander in a written or electronic format in a manner prescribed by the cognizant District Commander.

(c) The FSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the FSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.